PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-101568
(43)Date of publication of application : 07.04.2000

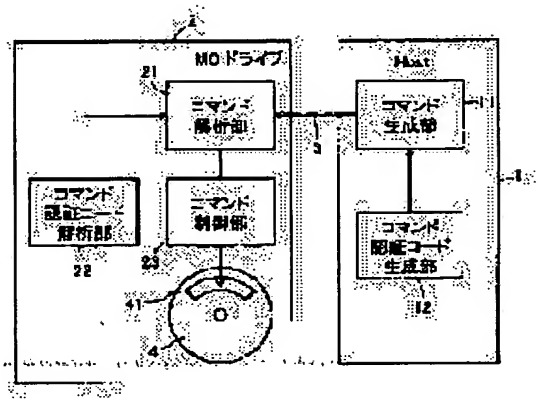
(51)Int.Cl. H04L 9/32
G06F 12/14
G06F 15/00
G11B 20/10

(21)Application number : 10-265211
(22)Date of filing : 18.09.1998

(71)Applicant : FUJITSU LTD
(72)Inventor : HIRANO HIDEYUKI
HASEBE TAKAYUKI
KOTANI MASATAKE

(54) COMMAND AUTHENTICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a command authentication method for preventing a command issued from a third person from setting itself up as the command by a normal user and maintaining high security.
SOLUTION: An authentication code in the command transmitted from a host 1 is collated by a command authentication code analysis part 22, and in the case of matching with information for collation, a specified command is generated by a command analysis part 21 and executed by a command control part 23. The specified command is executed based on authentication information in the command, it is difficult to analyze the authentication information and the high security is maintained.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2000－101568
(P2000－101568A)
(43)公開日　平成12年4月7日(2000.4.7)

(51)Int.Cl.'		識別記号	FI			テーマコード'(参考)
H04L	9/32		H04L	9/00	675A	5B017
G06F	12/14	320	G06F	12/14	320C	5B085
	15/00	330		15/00	330C	5D044
G11B	20/10		G11B	20/10	D	5J104
			H04L	9/00	673A	

審査請求　未請求　請求項の数11　OL　(全 6 頁)

(21)出願番号　特願平10－265211

(22)出願日　平成10年9月18日(1998.9.18)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中4丁目1番1号

(72)発明者　平野　秀幸
神奈川県川崎市中原区上小田中4丁目1番1号　富士通株式会社内

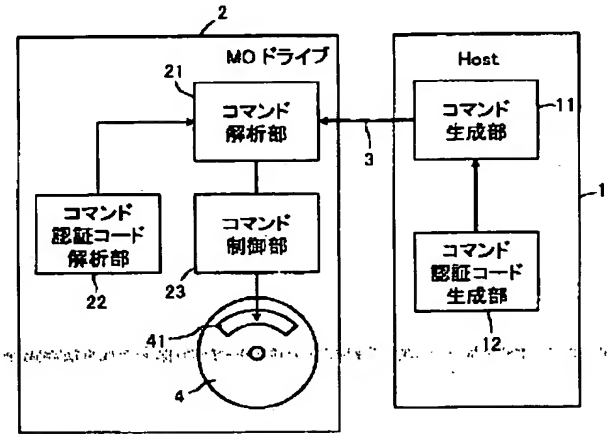
(72)発明者　長谷部　高行
神奈川県川崎市中原区上小田中4丁目1番1号　富士通株式会社内

(74)代理人　100094145
弁理士　小野　由己男　(外2名)

最終頁に続く

(54)【発明の名称】　コマンド認証方法

(57)【要約】
【課題】　第3者から発行されたコマンドが正規のユーザによるコマンドになりすますことを防止し、高いセキュリティを維持するコマンド認証方法を提案する。
【解決手段】　ホスト1から送信されてきたコマンド中の認証コードをコマンド認証コード解析部22によって照合し、照合用情報と合致した場合にはコマンド解析部21によって特定のコマンドを生成してコマンド制御部23に実行させる。



1

【特許請求の範囲】
【請求項１】受信したコマンドから認証情報を抽出し、前記認証情報を照合用情報と比較して合致した場合に対応するコマンドを実行するコマンド認証方法。
【請求項２】受信したコマンド中に格納された認証コードから認証情報を抽出する、請求項１に記載のコマンド認証方法。
【請求項３】前記認証コードは非繰り返し数であり、送信側から前記コマンドを送信する際に送信毎に前記認証コードの更新が行われる、請求項２に記載のコマンド認証方法。
【請求項４】前記認証コードは時刻情報または乱数により生成される、請求項３に記載のコマンド認証方法。
【請求項５】前記認証コードは座標アドレスを有する乱数系列表を用いて生成され、送信側から前記コマンドを送信する際に送信毎に座標アドレスを更新することによって前記認証コードの更新が行われる、請求項４に記載のコマンド認証方法。
【請求項６】受信したコマンド中に格納された複数の認証コードから認証情報を抽出する、請求項２に記載のコマンド認証方法。
【請求項７】受信したコマンドの引数が、前記認証コードまたは認証コードから生成された鍵により暗号化されている、請求項２に記載のコマンド認証方法。
【請求項８】受信したコマンド中に格納された認証コードを抽出してこれを時系列に配列された認証情報とし、前記照合用情報と一致した場合に特定のコマンドを実行する、請求項２に記載のコマンド認証方法。
【請求項９】受信したコマンド中に格納された認証コードを抽出してこれを時系列に配列された認証情報とし、前記照合用情報と一致した場合にコマンドの引数を追加変更して実行する、請求項２に記載のコマンド認証方法。
【請求項１０】受信したコマンド中に格納された認証コードを抽出し、時系列に受信したコマンドの実行を途中で終了した場合、コマンド送受信間の信号を特定状態とする、請求項２に記載のコマンド認証方法。
【請求項１１】受信したコマンド中に格納された認証コードを抽出し、この認証コードを特定の記憶領域に保存しておく、請求項８～１０のいずれかに記載のコマンド認証方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、コマンド認証方法、特に、コンピュータなどの外部機器から送信されてくるコマンドを正規のものであるか否かを判別するためのコマンド認証方法に関する。
【０００２】
【従来の技術】ユーザが任意のデータを書き込むことが可能な記録媒体として、光磁気ディスク（ＭＯ）、ディジタルビデオディスク（ＤＶＤ）、フロッピーディスク（ＦＤ）、ミニディスク（ＭＤ）などがある。このような記録媒体を駆動するためのドライブは、ＳＣＳＩインターフェイスなどを介してコンピュータと接続されており、コンピュータから送信されてくるコマンドにより、記録媒体上のデータの書き込み、読み出しが行われる。
【０００３】通常、記録媒体は、媒体固有番号を格納している第１階層、特定の情報を格納しておく第２階層、任意の電子化データを格納する第３階層を備えている。第１階層はデータの読み出しは可能であるが書き換えが不可能な領域であり、第２階層はユーザによる読み出し・書き換えが不可能な領域である。また、第３階層は、ユーザが自由に利用できる領域である。
【０００４】たとえば、コンピュータプログラムや電子出版物などの電子化データの著作権を保護するために、これら電子化データを所定の暗号鍵で暗号化して第３階層に格納しておくことが考えられる。この場合、第３階層に格納した電子化データの利用権に基づく許諾情報を第２階層に格納しておき、この許諾情報に基づいて正規のユーザが電子化データを復号化して利用することができるようにすることが考えられる。このとき、電子化データを格納した記録媒体を配布する際に、復号化するための鍵を許諾情報として第２階層に予め格納しておくことが可能である。また、記録媒体上に格納された電子化データを利用するための利用権をユーザが後に入手した場合に、第２階層にある許諾情報を所定のデータに置き換えて電子化データの復号化を行うように構成してもよい。
【０００５】このようにした場合、ユーザはコンピュータ側から特定のコマンドを送信し、第２階層に格納されている所定の情報を読み出したり、書き込んだりする必要がある。この記録媒体の第２階層は、通常はユーザによる書き込み・読み出しが不可能な領域であるため、特定のコマンドが正規のユーザによるものかどうかを判別して実行する必要がある。従来では、ユーザのパスワードを設定しておき、コンピュータ側から特定のコマンドを送出する際に、このコマンドをパスワードに関係付けて送信するように構成している。
【０００６】
【発明が解決しようとする課題】上述のようにした場合、パスワードに関するコマンドが独立してコマンドを認証することにより、特定のコマンドが正規のユーザによるものか否かを判別している。しかしながら、第３者によってこのパスワードに関するコマンドを解析されると、特定のコマンドを発行することが可能となり、セキュリティレベルが低下する。特に、コンピュータとドライブとの間のデータバスはモニタすることが可能であり、コンピュータから送出されるコマンドを解析することによってパスワードを入手することは比較的簡単であると考えられる。

2

【０００７】本発明は、第３者から発行されたコマンドが正規のユーザによるコマンドになりすますことを防止し、高いセキュリティを維持するコマンド認証方法を提案する。

【０００８】

【課題を解決するための手段】本発明に係るコマンド認証方法は、受信したコマンドから認証情報を抽出し、認証情報を照合用情報と比較して合致した場合に対応するコマンドを実行する。ここで、受信したコマンド中に格納された認証コードから認証情報を抽出するように構成できる。

【０００９】また、認証コードは非繰り返し数であり、送信側からコマンドを送信する際に送信毎に認証コードの更新が行われるように構成できる。さらに、認証コードは時刻情報または乱数により生成されたものとすることができる。　このとき、認証コードは座標アドレスを有する乱数系列表を用いて生成され、送信側からコマンドを送信する際に送信毎に座標アドレスを更新することによって認証コードの更新が行われるように構成できる。

【００１０】また、受信したコマンド中に格納された複数の認証コードから認証情報を抽出する。さらに、受信したコマンドの引数が、認証コードまたは認証コードから生成された鍵により暗号化されたものとすることができる。また、受信したコマンド中に格納された認証コードを抽出してこれを時系列に配列された認証情報とし、照合用情報と一致した場合に特定のコマンドを実行するように構成できる。

【００１１】また、受信したコマンド中に格納された認証コードを抽出してこれを時系列に配列された認証情報とし、照合用情報と一致した場合にコマンドの引数を追加変更して実行するように構成できる。さらに、受信したコマンド中に格納された認証コードを抽出し、時系列に受信したコマンドの実行を途中で終了した場合、コマンド送受信間の信号を特定状態とすることができる。

【００１２】また、受信したコマンド中に格納された認証コードを抽出し、この認証コードを特定の記憶領域に保存しておくように構成できる。

【００１３】

【発明の実施の形態】本発明の１実施形態について図を参照して説明する。図１は、装置構成を示す概略ブロック図である。ここでは、パソコンとMOドライブとがＳＣＳＩケーブルにより接続されている場合を考える。図１において、ホスト１とMOドライブ２とはデータバス３を介して接続されている。ホスト１は、コマンドの送信側であって、ＣＰＵ、ＲＯＭ、ＲＡＭ、各種インターフェイスなどを備える、いわゆるパーソナルコンピュータである。ホスト１は、コマンド生成部１１とコマンド認証コード生成部１２とを有している。コマンド生成部１１は、MOドライブ２に送信する各種コマンドを生成する。コマンド認証コード生成部１２は、コマンド生成部１１で生成されるコマンドが特定のコマンドである場合に、認証情報を付加するために認証コードを生成するものである。

【００１４】MOドライブ２は、光磁気ディスク４を駆動するものであって、ホスト１から送信されてくるコマンドに従って、光磁気ディスク４に電子化データを書き込み、また光磁気ディスク４に格納されている電子化データを読み出す。このMOドライブ２も、ＣＰＵ、ＲＯＭ、ＲＡＭ、入出力インターフェイスなどを備えている。MOドライブ２は、コマンド解析部２１、コマンド認証コード解析部２２、コマンド制御部２３を有している。コマンド解析部２１は、ホスト１から送信されてくるコマンドをその引数などを含めて解析し、対応するコマンドを発行する。コマンド認証コード解析部２２は、送信されてきたコマンドが認証コード付きである場合に、この認証コードを解析して照合用情報と照合し、照合した結果をコマンド解析部２１に送信する。コマンド制御部２３は、コマンド解析部２１から発行されたコマンドに従って、光磁気ディスク４の電子化データを書き込みあるいは読み出しなどの制御を行う。

【００１５】ここで、光磁気ディスク４のセキュリティ領域４１は、通常ユーザによるアクセスが不可能な領域であるが、コマンド解析部２１が特定のコマンドを発行した場合にのみ、このセキュリティ領域４１の内容にアクセスできるものとする。ホスト１では、コマンド解析部２１が特定のコマンドを発行するために、特定のコマンドを特定の認証コードに関連付けて送出することとなる。

【００１６】以下に、具体的な実施形態を説明する。

〔第１実施形態〕第１実施形態では、乱数により認証コードを生成する場合を示す。ホスト１およびMOドライブ２に、図２に示すような２つの共通する乱数系列表５１，５２を用意する。この乱数系列表５１，５２の表番号（Ａ）は、それぞれ０，１である。また、乱数系列表５１，５２は、それぞれ２次元座標のアドレスを備えており、アドレスポインタ（Ｘｉ，Ｙｊ）で表されるアドレスにはそれぞれ１６進数で表現される１バイトの乱数が格納されている。

【００１７】ホスト１側では、図３に示すようなコマンド６０をコマンド生成部１１で生成する。コマンド６０は、オペコード６１と、このオペコード６１に関係する引数６２と、オペランドの一部に格納される認証コード６３とからなっている。認証コードは、コマンド認証コード生成部１２によって生成されるものであり、ここでは、乱数系列表５１，５２のうちのどちらを選択したかを示す表番号（Ａ）と、選択した乱数系列表の座標を示すアドレスポインタ（ｘ，ｙ）となる。

【００１８】このような乱数系列表を用いて認証コード付きのコマンドを送受信する場合には、図４に示すよう

な手順で実行される。まず、ホスト１から初期設定として乱数系列表の開始アドレスを送信する。ＭＯドライブ２では、この開始アドレスを受信して、乱数系列表の初期アドレスの設定を行う。ホスト１から特定のコマンドを発行する場合には、コマンド認証コード生成部１２により表番号（Ａ）およびアドレスポインタ（ｘ，ｙ）による認証番号を生成し、さらにこれを通常のコマンドに付加した認証コード付きコマンド６０を生成して、ＭＯドライブ２に送信する。ＭＯドライブ２側では、コマンド６０のオペランドに格納されている認証コード６３を解析して、この認証コード６３に基づく乱数系列表の乱数の値を、ＭＯドライブ２側の現在のアドレスポインタによる乱数の値と比較する。この結果が一致した場合には、コマンド解析の結果が正常であった旨の報告をホスト１に送信し、ホスト１では処理を終了する。また、ＭＯドライブ２側では、コマンド６０に基づく特定のコマンドを発行し、光磁気ディスク４に対する制御を行う。コマンド解析の結果、乱数の値が一致しない場合には、異常フラグをホスト１に送信する。ホスト１側で異常フラグを受信した場合には、再度認証コード付きのコマンドを生成してＭＯドライブ２に送信する。ＭＯドライブ２では、認証コード付きコマンドを受信し、上述と同様の動作を繰り返す。

【００１９】このように構成した場合、ホスト１が認証コード付きコマンドをＭＯドライブ２に送信する毎に、認証コードが毎回更新されるので、時系列的なコマンドの送受信をすべてモニタしない限り特定のコマンドを発行させることは困難であり、セキュリティを高く維持することが可能である。２つの乱数系列表を用いて乱数による認証コードを生成したが、１つの乱数系列表だけであってもよく、また、３以上の乱数系列表を用いて認証コードを生成するように構成することも可能である。

〔第２実施形態〕コマンドに付随する引数が特定の鍵によって暗号化されている場合を第２実施形態として示す。

【００２０】ホスト１では、図５に示すように、認証コード付きコマンド７０を生成する。このコマンド７０は、オペコード７１と、特定の鍵によって暗号化された第１引数７２と、第２引数７３と、認証コード７４とで構成されている。認証コード７４は、たとえば、前述したような乱数系列表を用いて、表番号（Ａ）とアドレスポインタ（ｘ，ｙ）でなるコードとすることができる。第１引数７２は、認証コード７４で示される乱数系列表の対応する乱数を鍵として暗号化されている。

【００２１】このようなコマンド７０を受信したＭＯドライブ２側の動作を図６のフローチャートにより説明する。ステップＳ１では、認証コード７４を解析する。ここでは、乱数系列表を参照して現在のアドレスポインタによる乱数の値が一致しない場合には、異常フラグをホスト１側に送信してエラー処理を行い、値が一致した場合にはステップＳ２に移行する。ステップＳ２では、認証コード７４に基づく復号鍵を生成し、これを所定の領域に格納する。

【００２２】ステップＳ３では、オペコード７１をデコードする。ステップＳ４では、認証コード７４に基づく復号鍵により第１引数７１を復号化する。ステップＳ５では、コマンドを実行する。この第２実施形態では、第１引数７２が暗号化されているため、よりセキュリティを高く維持することができる。

【００２３】第２引数７３も同様に暗号化して格納することも可能である。

〔第３実施形態〕複数の認証コードを用いる場合について、第３実施形態として説明する。ホスト１では、図７に示すように、認証コード付きコマンド８０を生成する。このコマンド８０は、オペコード８１と、引数８２と、第１認証コード８３と、第２認証コード８４とで構成されている。第１認証コード８３と第２認証コード８４は、この２つからコマンドの認証を行うための認証コードを生成できるように構成されており、たとえば、２つの認証コードから上述した乱数系列表の次のアドレスポインタを生成するような構成、２つの認証コードにうち一方が暗号化された情報であり他方が復号化する復号鍵であるような構成などが考えられる。

【００２４】このようなコマンド８０を受信したＭＯドライブ２側の動作を図８のフローチャートにより説明する。ステップＳ１１では、第１認証コード８３および第２認証コード８４を読み出す。ステップＳ１２では、読み出した第１認証コード８３および第２認証コード８４から認証コードを生成する。たとえば、２つの認証コード８３，８４に基づいて乱数系列表を参照する、一方のコードを他方のコードで復号化するなどして認証コードを生成する。ステップＳ１３では、生成した認証コードを解析して、一致しない場合には、異常フラグをホスト１側に送信してエラー処理を行い、値が一致した場合にはステップＳ１４に移行する。

【００２５】ステップＳ１４では、オペコード８１をデコードする。ステップＳ１５では、コマンドを実行する。このようにした第３実施形態によれば、第１認証コードおよび第２認証コードから実際の認証コードを生成するためのアルゴリズムを入手することが困難であり、さらに高いセキュリティを維持することが可能となる。

〔第４実施形態〕時系列に受信したコマンド列によって特定のコマンドを発行する場合について、第４実施形態として説明する。

【００２６】ホスト１では、図９に示すように、認証コード付きコマンド９０を生成する。このコマンド９０は、オペコード９１と、第１引数９２と、第２引数９３と、認証コード９４とで構成されている。ＭＯドライブ２側では、複数のコマンド列を受信した際に、それぞれの認証コード９４を時系列として、特定のパターンであ

るか否かを判別し、特定のパターンであった場合にのみ、特定のコマンドを発行するように構成する。

【００２７】たとえば、同一のコマンドＡを３個連続して受信した場合に、各コマンドに格納された認証コードが一定のパターンである場合に特定のコマンドを発行するように構成できる。図１０に示すように、同一のコマンドＡを３個連続して受信した場合、それぞれコマンドに格納された認証コードＣ１，Ｃ２，Ｃ３を抽出する。この認証コード列が予めＭＯドライブ２側で用意したテーブルに合致していれば、特定のコマンドを発行する。

【００２８】また、図１１に示すように、異なるコマンドＡ，Ｂ，Ｃを順に受信した場合に、各コマンドに格納された認証コードが一定のパターンである場合に特定のコマンド発行する構成とすることができる。図１１に示すように、異なるコマンドＡ，Ｂ，Ｃをこの順に受信した場合に、それぞれのコマンドに格納された認証コードＣ１，Ｃ２，Ｃ３を抽出する。この認証コード列が予めＭＯドライブ２側で用意したテーブルに合致していれば、特定のコマンドを発行する。

【００２９】このようにした場合には、特定のコマンドを発行するために、複数のコマンドおよび認証コードを必要とし、不正なコマンド制御を防止することができる。複数のコマンドを受信した後、コマンドの実行が途中で終了した場合には、ＭＯドライブ２に格納されている認証コードとキャッシュをクリアするように構成することができる。このことにより、コマンドを受信した際にハッキングが発生しても、認証コードを盗まれることを防止できる。

【００３０】また、時系列で受信したコマンドに格納された認証コードを監査情報として順に保存しておく構成とすることができる。この場合には、認証コードの配列またはその個数によりＭＯドライブ２への不正が行われたか否かを知ることができる。上述した各実施形態において、光磁気ディスク（ＭＯ）に代えて、ディジタルビデオディスク（ＤＶＤ）、ミニディスク（ＭＤ）、フロッピーディスク（ＦＤ）、ハードディスク（ＨＤ）その他の記録媒体に適用することができる。

【００３１】

【発明の効果】本発明によれば、コマンド中の認証情報に基づいて特定のコマンドを実行するように構成しており、認証情報を解析することが困難であり、高いセキュリティを維持することが可能となる。

【図面の簡単な説明】

【図１】装置構成を示す概略ブロック図。

【図２】乱数系列表の説明図。

【図３】第１実施形態に用いられるコマンドの説明図。

【図４】第１実施形態の信号の流れを示す説明図。

【図５】第２実施形態に用いられるコマンドの説明図。

【図６】第２実施形態の制御フローチャート。

【図７】第３実施形態に用いられるコマンドの説明図。

【図８】第３実施形態の制御フローチャート。

【図９】第４実施形態に用いられるコマンドの説明図。

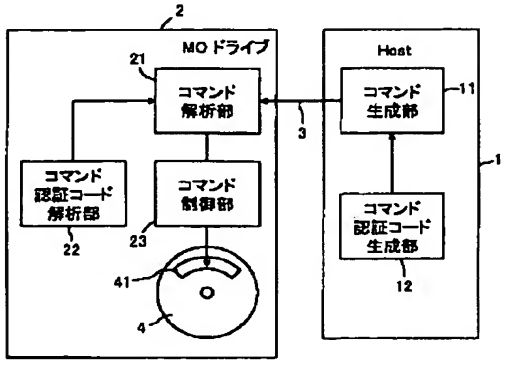
【図１０】受信するコマンドの時系列説明図。

【図１１】受信するコマンドの時系列説明図。

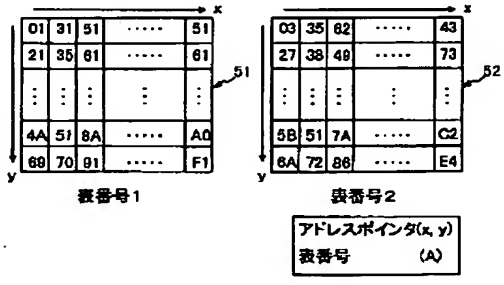
【符号の説明】

１　ホスト
２　ＭＯドライブ
３　データバス
４　光磁気ディスク
１１　コマンド生成部
１２　コマンド認証コード生成部
２１　コマンド解析部
２２　コマンド認証コード解析部
２３　コマンド制御部
４１　セキュリティ領域
５１　乱数系列表
５２　乱数系列表

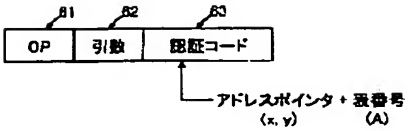
【図１】



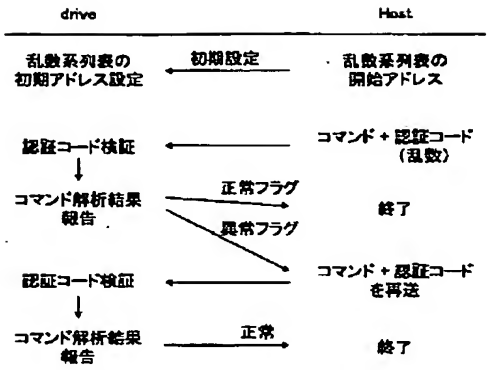
【図２】



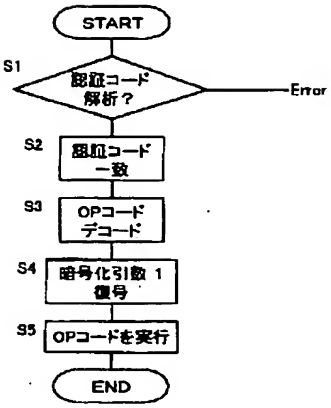
【図３】



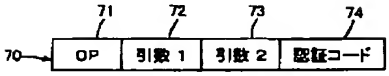
【図４】



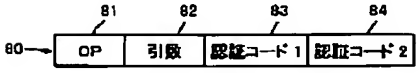
【図６】



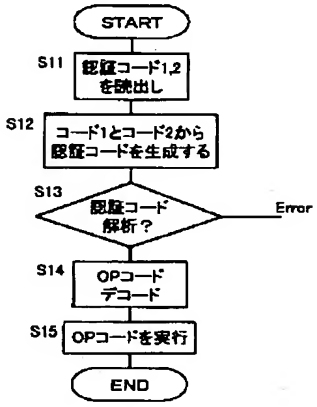
【図５】



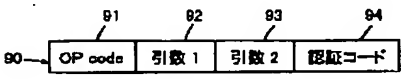
【図７】



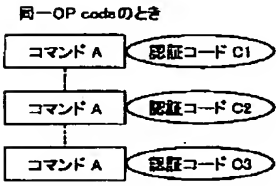
【図８】



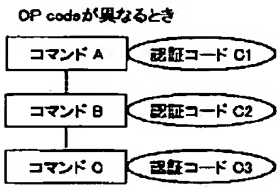
【図９】



【図１０】



【図１１】



フロントページの続き

(72)発明者　小谷　誠剛
神奈川県川崎市中原区上小田中４丁目１番
１号　富士通株式会社内

Ｆターム(参考)　5B017 AA07 BA05 BB02 CA09
5B085 AC03 AE06 AE23 AE29 CC11
CC16
5D044 BC01 BC02 CC04 DE42 DE48
HL02 HL11
5J104 AA07 AA12 GA03 GA05 KA01
NA04 NA32 NA38